

ON MAXIMAL CURVES WHICH ARE NOT GALOIS SUBCOVERS OF THE HERMITIAN CURVE

IWAN DUURSMA AND KIT-HO MAK

ABSTRACT. We show that the generalized Giulietti-Korchmáros curve defined over $\mathbb{F}_{q^{2n}}$, for $n \geq 3$ odd and $q \geq 3$, is not a Galois subcover of the Hermitian curve over $\mathbb{F}_{q^{2n}}$. This answers a question raised by Garcia, Güneri and Stichtenoth.

1. INTRODUCTION AND STATEMENTS OF RESULTS

Let \mathbb{F}_{q^2} be the finite field with q^2 elements, and let \mathcal{X} be a projective, nonsingular, geometrically irreducible curve (hereafter referred to as a *curve*) defined over \mathbb{F}_{q^2} . We say that \mathcal{X} is \mathbb{F}_{q^2} -maximal if the number of its rational points attains the Hasse-Weil upper bound

$$|\mathcal{X}(\mathbb{F}_{q^2})| = q^2 + 1 + 2g(\mathcal{X})q,$$

where $g(\mathcal{X})$ is the genus of \mathcal{X} . The most important example of a maximal curve is the Hermitian curve \mathcal{H} , which is defined over \mathbb{F}_{q^2} by the equation

$$y^q + y = x^{q+1}.$$

It has genus $\frac{1}{2}q(q-1)$. By the work of [8, 15, 26], the genus of any maximal curve \mathcal{X} satisfies

$$g(\mathcal{X}) \in [0, (q-1)^2/4] \cup \{q(q-1)/2\}.$$

Therefore the Hermitian curve has the largest possible genus that a maximal curve can have. It is shown in [21] that the Hermitian curve is the unique maximal curve having genus $\frac{1}{2}q(q-1)$. More information about maximal curves can be found in [2, 3, 7, 9, 13, 16, 17] and their references.

A curve \mathcal{C} is called a *subcover* of \mathcal{X} over \mathbb{F}_{q^2} (or equivalently \mathcal{X} is a *cover* of \mathcal{C}) if there exists a surjective map $\phi : \mathcal{X} \rightarrow \mathcal{C}$ with \mathcal{C} , \mathcal{X} and ϕ defined over \mathbb{F}_{q^2} . By a result known as Serre's theorem (see [18, Proposition 6]), any subcover of a \mathbb{F}_{q^2} -maximal curve is \mathbb{F}_{q^2} -maximal. Most of the known maximal curves are subcovers of the Hermitian curve \mathcal{H} , and systematic studies on subcovers of \mathcal{H} can be found in [4, 5, 12].

The first example of a maximal curve which is not a Galois subcover of the Hermitian curve is the curve $y^9 - y = z^7$ over \mathbb{F}_{36} discovered by Garcia and Stichtenoth [11]. It is the special case with $q = 3$, $n = 3$ of the curve \mathcal{X}_n with defining equation

$$(1.1) \quad y^{q^2} - y = z^{\frac{q^n+1}{q+1}}$$

2010 *Mathematics Subject Classification.* Primary 11G20; Secondary 14G15, 14H25.

Key words and phrases. maximal curves, generalized GK curves, Galois coverings.

over $\mathbb{F}_{q^{2n}}$, for $q \geq 2$ and odd $n \geq 3$. The curve \mathcal{X}_n was shown to be maximal in [1]. As another example, an unpublished calculation by Rains and Zieve states that the Ree curve of genus $g = 15$ over \mathbb{F}_{3^6} is not a Galois subcover of the Hermitian curve over the same field.

In [13], Giulietti and Korchmáros give an example of a maximal curve, now called the GK curve, that is not covered by the Hermitian curve. The GK curve has been generalized by Garcia, Güneri and Stichtenoth in [10]. The generalized GK curves \mathcal{C}_n are maximal curves over $\mathbb{F}_{q^{2n}}$ for a prime power q and odd $n \geq 3$ ([10], see also [6]). They have defining equations

$$(1.2) \quad \begin{aligned} x^q + x &= y^{q+1} \\ y^{q^2} - y &= z^{\frac{q^n+1}{q+1}}. \end{aligned}$$

It is shown in [10] that the curves with $n = 3$ are isomorphic to those given originally by Giulietti and Korchmáros. It is not known whether these generalized GK curves \mathcal{C}_n are covered by the Hermitian curve for $n \geq 5$. In this paper, we give a partial answer to this problem by showing that \mathcal{C}_n is not a Galois subcover of the Hermitian curve over the same finite field for any odd $n \geq 3$ and $q \geq 3$. More precisely, we prove the following.

Theorem 1.1. *The generalized GK curve, defined by (1.2) over $\mathbb{F}_{q^{2n}}$, is not a Galois subcover of the Hermitian curve over $\mathbb{F}_{q^{2n}}$ for any $q \geq 3$ and odd $n \geq 3$.*

For the proof we make use of the Artin character for the Hermitian function field. This appears to be the first time that the Artin character is used to study subcovers of the Hermitian function field and it allows us to avoid dealing with explicit equations and group structures for Galois subcovers. The proof depends on Proposition 5.1 which may be of independent interest and which gives a new lower bound for the degree of a Galois covering $\phi : \mathcal{X} \rightarrow \mathcal{C}$ of a maximal curve \mathcal{C} by a Hermitian curve \mathcal{X} .

For $q = 2$, the situation is different. For the case $n = 3$, Giulietti and Korchmáros show that the GK curve over \mathbb{F}_{64} is covered by the Hermitian curve over the same field [13]. We prove that if the generalized GK curve \mathcal{C}_n over $\mathbb{F}_{2^{2n}}$ is Galois covered by the Hermitian curve over $\mathbb{F}_{2^{2n}}$, then there is exactly one possibility for the degree and ramification structure.

Theorem 1.2. *Let $n \geq 5$ be an odd integer. If the generalized GK curve, defined by (1.2) with $q = 2$ over $\mathbb{F}_{2^{2n}}$, is Galois covered by the Hermitian curve over the same finite field, then the degree of the covering is $d = (2^n + 1)/3$, and the covering is unramified.*

Next, we consider the curve \mathcal{X}_n defined over $\mathbb{F}_{q^{2n}}$ by (1.1) which is the second equation in the definition of the generalized GK curve. For $q = 2$ it is shown in [1] that \mathcal{X}_n is covered by the Hermitian curve, but it is not known whether this curve is a subcover of the Hermitian curve for $q \geq 3$. For $q = 3$, Garcia and Stichtenoth [11] showed that the curve is not a Galois subcover of the Hermitian curve. Unlike the case for the generalized GK curve, our new lower bound does not eliminate all the possible degrees of a Galois covering. Nevertheless, we are able to shorten the interval of possible degrees that is obtained by the traditional method (which will be outlined in Section 2).

Theorem 1.3. *Let $n \geq 3$ be an odd integer. If the curve \mathcal{X}_n defined by (1.1) with $q > 2$ is Galois covered by the Hermitian curve over the same finite field, then the degree of the covering d satisfies*

$$\frac{(q+1)(q^n+1)}{q^2+1} \leq d \leq q^{n-1} + q^{n-2} + \dots + q^2 + q + 2.$$

We remark that for $n \geq 5$, we do not know whether the curve \mathcal{C}_n is non-Galois covered by the Hermitian curve or not.

2. SUBCOVERS OF THE HERMITIAN CURVE

Let \mathcal{H}_n be the Hermitian curve of degree $q^n + 1$ over $\mathbb{F}_{q^{2n}}$. It has genus $g(\mathcal{H}_n) = \frac{1}{2}q^n(q^n - 1)$ and number of $\mathbb{F}_{q^{2n}}$ -rational points $N(\mathcal{H}_n) = q^{3n} + 1$. Let \mathcal{Y}_n be a subcover of the Hermitian curve with morphism $\phi : \mathcal{H}_n \rightarrow \mathcal{Y}_n$ of degree d . From the splitting of points we obtain a lower bound for d , and from the Hurwitz genus formula (see [25, Theorem 3.4.13]) an upper bound for d ,

$$(2.1) \quad \frac{N(\mathcal{H}_n)}{N(\mathcal{Y}_n)} \leq d \leq \frac{2g(\mathcal{H}_n) - 2}{2g(\mathcal{Y}_n) - 2}.$$

Subcovers of the Hermitian curve are again maximal, and thus

$$N(\mathcal{Y}_n) = q^{2n} + 1 + 2g(\mathcal{Y}_n)q^n = (q^n + 1)^2 + (2g(\mathcal{Y}_n) - 2)q^n.$$

The Hermitian curve has $2g(\mathcal{H}_n) - 2 = (q^n - 2)(q^n + 1)$. For $(A - 1)(q^n + 1) \leq 2g(\mathcal{Y}_n) - 2 < A(q^n + 1)$, the bounds (2.1) yield

$$\frac{q^n}{A + 1} \leq d \leq \frac{q^n - 2}{A - 1}.$$

The lower bound holds with equality for a covering $\phi : \mathcal{H}_n \rightarrow \mathcal{Y}_n$ of degree d with

$$(2.2) \quad 2g(\mathcal{Y}_n) - 2 = (q^n/d - 1)(q^n + 1) - (q^n/d + 1) \quad \text{for } d|q^n.$$

Such a covering exists for every divisor d of q^n ([12, Section 3]). For other cases we will use the following refinement of the lower bound.

Lemma 2.1. *Let \mathcal{Y}_n be a maximal curve with $2g(\mathcal{Y}_n) - 2 = A(q^n + 1) - B$, for integers A and B with $1 \leq B \leq q^n + 1$. For $k(A + 1) < B$, and for $B \neq A + 2$,*

$$\frac{q^n + k}{A + 1} \leq d.$$

In particular, $d(A + 1) \geq q^n + 1$ for $B > A + 2$.

Proof. For the relevant case $B = k(A + 1) + 1$, the inequality $N(\mathcal{H}_n)(A + 1) > N(\mathcal{X}_n)(q^n - 1 + k)$ reduces to $(kq^n - 1)(k - 2) + A + A(k - 1)^2 q^n > 0$, which holds for $k \geq 2$ and for $k = 0$. For $k = 1$, we need to verify only the case $B = A + 3$. For $B = A + 3$, the inequality $N(\mathcal{H}_n)(A + 1) > N(\mathcal{X}_n)(q^n)$ reduces to $q^{2n} - q^n + A + 1 > 0$. \square

Let k be maximal with $k(A+1) < B$. For the degree of the ramification divisor R we write

$$(2.3) \quad \deg R = (2g(\mathcal{H}_n) - 2) - d(2g(\mathcal{Y}_n) - 2) = R_0(q^n + 1) + R_1,$$

where $R_0 = (q^n - 2 - dA + k)$ and $R_1 = dB - k(q^n + 1)$. For Galois subcovers, we write the degree of the ramification divisor in a different way in the next two sections. In Proposition 5.1 we show that the combined descriptions exclude the possibility $R_1 < q^n + 1$, which yields a lower bound $d \geq (k+1)(q^n + 1)/B$ that in many cases improves the standard lower bound (2.1).

3. THE DEGREE OF THE RAMIFICATION DIVISOR OF A GALOIS COVERING

Now we suppose that the covering $\phi : \mathcal{H}_n \rightarrow \mathcal{Y}_n$ is Galois with Galois group G , with $|G| = d$. Then G can be realized as a subgroup of $\text{Aut}(\mathcal{H}_n) = \text{PGU}(3, q^n)$ (see [20, 24]), and \mathcal{Y}_n is the quotient curve of \mathcal{H}_n by G . To understand the ramification in a Galois covering, we will use the Hilbert different formula (see the proof in [25, Theorem 3.8.7]), which we state here for the sake of completeness. Let $\mathcal{X} \rightarrow \mathcal{X}'$ be a Galois covering of curves with Galois group G , and let P and P' be points on \mathcal{X} and \mathcal{X}' respectively (which need not lie in the field of definition of the covering) so that P maps to P' under the covering. Then the different exponent $d(P|P')$ is

$$(3.1) \quad d(P|P') = \sum_{\substack{1 \neq \sigma \in G \\ \sigma(P)=P}} i_P(\sigma),$$

where $i_P(\sigma) = v_P(\sigma(t) - t)$ with t a local uniformizer at P . Note that if the ramification of P over P' is tame, then $i_P(\sigma) = 1$ for any σ that fixes P , and in that case $d(P|P')$ is the number of elements $\sigma \neq 1$ in G that fix P . For any $\sigma \in \text{PGU}(3, q^n)$, define

$$(3.2) \quad i(\sigma) := \sum_{P \in \mathcal{X}} i_P(\sigma) \deg P,$$

with the convention that $i_P(\sigma) = 0$ if $\sigma(P) \neq P$. Combining (3.1) with the Hurwitz genus formula, we get the following proposition which we will rely on heavily.

Proposition 3.1. *Suppose $\mathcal{X} \rightarrow \mathcal{X}'$ is a Galois covering of degree d with Galois group G , then*

$$2g(\mathcal{X}) - 2 = d(2g(\mathcal{X}') - 2) + \deg R,$$

where R is the ramification divisor, whose degree is given by

$$\deg R = \sum_{1 \neq \sigma \in G} i(\sigma).$$

Remark 3.2. We want to point out the relation between $i(\sigma)$ and the Artin representation (see [22, Chapter 19], [23, Chapter VI]). The character of the Artin representation satisfies $a(\sigma) = -i(\sigma)$, for $\sigma \neq 1$, and $\sum_{\sigma} a(\sigma) = 0$. For the subcover of the Hermitian function field with group $\text{PGU}(3, q^n)$, the Artin representation is the unique irreducible representation of minimal degree $2g(\mathcal{H}_n) = q^n(q^n - 1)$ (see [19, Lemma 4.1]).

4. ARTIN CHARACTER OF THE HERMITIAN FUNCTION FIELD

To apply Proposition 3.1 with $\mathcal{X} = \mathcal{H}_n$ and $\mathcal{X}' = \mathcal{Y}_n$, we need to understand the values of $i(\sigma)$ defined by (3.2) for $\sigma \in PGU(3, q^n)$. The action of $PGU(3, q^n)$ on the Hermitian curve \mathcal{H}_n is well-known [24]. An element in $PGU(3, q^n)$ either fixes no points on \mathcal{H}_n , or it fixes a point of degree one, or fixes a point of degree three. If σ fixes no points on \mathcal{H}_n , then $i(\sigma) = 0$. If it fixes a point of degree three, then it fixes only that point. Since any such σ has order dividing $q^{2n} - q^n + 1$, which is relatively prime to q , the ramification is tame. Hence $i(\sigma) = 3$. The case when σ fixes a point of degree one has several subcases. Since the action of $PGU(3, q^n)$ on the points of degree one on \mathcal{H}_n is transitive (see for example [14]), and $i(\sigma)$ is unchanged under conjugation (see for example [23, Chapter IV]), we may assume that the degree one point fixed is the point at infinity P_∞ when \mathcal{H}_n is given by the equation $x^{q^n} + x = y^{q^n+1}$. Let H be the subgroup of $PGU(3, q^n)$ fixing P_∞ . One can show that H is of order $q^{3n}(q^{2n} - 1)$, and any $\sigma \in H$ is of the form

$$(4.1) \quad \sigma(x) = a^{q^n+1}x + ab^{q^n}y + c, \quad \sigma(y) = ay + b,$$

with $a \in \mathbb{F}_{q^{2n}} \setminus \{0\}$, $b \in \mathbb{F}_{q^{2n}}$, $c^{q^n} + c = b^{q^n+1}$. Following the notations in [12], we denote by $\sigma = [a, b, c]$ the automorphism $\sigma \in H$ given by (4.1). There are 2 cases.

Lemma 4.1. *Let P_∞ be the point at infinity when \mathcal{H}_n is given by the equation $x^{q^n} + x = y^{q^n+1}$, and let H be the subgroup of $PGU(3, q^n)$ fixing P_∞ . Let $\sigma = [a, b, c] \in H$ with $\sigma \neq 1$. For $a \neq 1$, we have*

$$i(\sigma) = \begin{cases} 1 & , \text{ if } p \text{ divides } \text{ord}(\sigma), \\ q^n + 1 & , \text{ if } \text{ord}(\sigma) \text{ divides } q^n + 1, \\ 2 & , \text{ otherwise.} \end{cases}$$

For $a = 1$, we have

$$i(\sigma) = \begin{cases} 2 & , \text{ if } a = 1, b \neq 0, \\ q^n + 2 & , \text{ if } a = 1, b = 0, c \neq 0. \end{cases}$$

Proof. (Case $a \neq 1$) The Sylow p -subgroup of H is the set consisting of $[a, b, c]$ with $a = 1$. Therefore, if $\sigma = [a, b, c]$ with $a \neq 1$, then σ is not in the higher ramification group of P_∞ , so it will not fix P_∞ to a high order. Since all other places is at most tamely ramified, we have

$$i_P(\sigma) = v_P(\sigma(t) - t) = \begin{cases} 0 & , \sigma(P) \neq P, \\ 1 & , \sigma(P) = P. \end{cases}$$

Therefore, in this case we have

$$i(\sigma) = \#\{P \in \mathcal{H}_n \mid \deg(P) = 1 \text{ and } \sigma(P) = P\}.$$

If $\text{ord}(\sigma)$ is a multiple of p , then σ cannot fix any degree one places other than P_∞ since those places are tame. Thus $i(\sigma) = 1$. Suppose now $\text{ord}(\sigma)$ divides $q^n + 1$, then one can show that $\sigma = [a, b, c]$ is conjugate in H to $\sigma^* = [a, 0, 0]$ (see [12, Lemma 4.1]). By (4.1), σ^* satisfies $\sigma^*(x) = x$ and $\sigma^*(y) = ay$. It is then easy to see that in the affine part of \mathcal{H}_n , σ^* fixes exactly the (affine) line $\{y = 0\}$. Hence, $i(\sigma^*) = q^n + 1$ as

$\#(\mathcal{H}_n \cap \{y = 0\}) = q^n$ and σ^* also fixes P_∞ . Since $i(\sigma)$ is preserved under conjugation, we have $i(\sigma) = i(\sigma^*) = q^n + 1$. Finally, if the order of σ does not divide $q^n + 1$, then again $\sigma = [a, b, c]$ is conjugate in H to $\sigma^* = [a, 0, 0]$. This time we have $\sigma^*(x) = a^{q^n+1}x$ and $\sigma^*(y) = ay$. So in the affine part of \mathcal{H}_n , σ^* fixes exactly the origin. Thus $i(\sigma) = i(\sigma^*) = 2$.

(Case $a = 1$) If $\sigma = [a, b, c]$ with $a = 1$, then σ is in the higher ramification group of P_∞ , and this is the only point that σ can fix. In this case, we compute $i(\sigma)$ directly from the definition. First, $i(\sigma) = i_{P_\infty}(\sigma) = v_{P_\infty}(\sigma(t) - t)$, where t is a local uniformizer at P_∞ . We choose $t = y/x$ to be the local uniformizer. Then

$$\begin{aligned} i(\sigma) &= v_{P_\infty}\left(\frac{y+b}{x+b^{q^n}y+c} - \frac{y}{x}\right) \\ &= v_{P_\infty}((y+b)x - y(x+b^{q^n}y+c)) - v_{P_\infty}(x) - v_{P_\infty}(x+b^{q^n}y+c) \\ &= v_{P_\infty}(-b^{q^n}y^2 + bx - cy) + 2(q^n + 1) \\ &= \begin{cases} 2 & , \text{ if } b \neq 0, \\ q^n + 2 & , \text{ if } b = 0, c \neq 0. \end{cases} \end{aligned}$$

□

The $i(\sigma)$ among various kinds of elements are shown in Figure 1. Each number in a box corresponds to a subgroup of that order, and each number on an edge is the $i(\sigma)$ for elements that lie in the upper group but not the lower one.

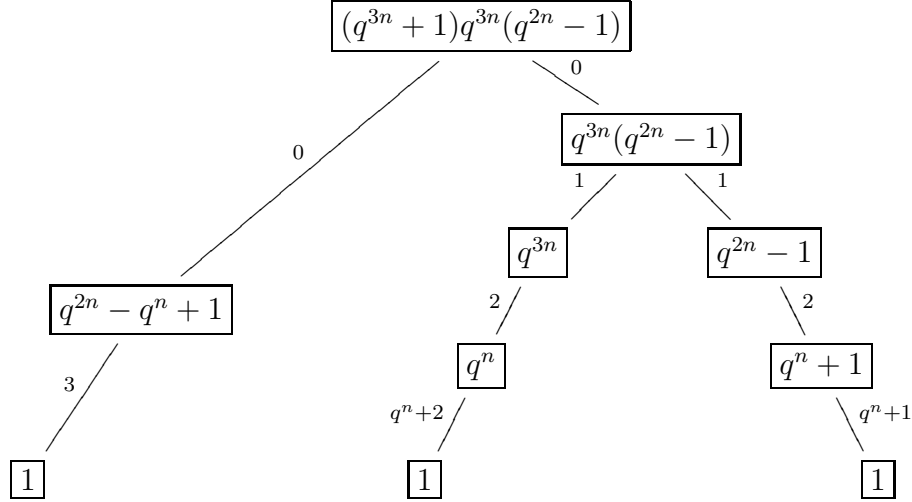


FIGURE 1. $i(\sigma)$ among various elements in $PGU(3, q^n)$

The following proposition follows immediately from the above lemma. The significance of the proposition is that either $i(\sigma)$ is very small, or $i(\sigma)$ is very large, and nothing in the middle can happen.

Proposition 4.2. *If $\sigma \in PGU(3, q^n)$, then $i(\sigma) = 0, 1, 2, 3, q^n + 1$ or $q^n + 2$.*

Now we have the contribution of each element in $PGU(3, q^n)$ to the ramification divisor, and we are ready to finish the proof of the theorems stated in the introduction.

5. GALOIS SUBCOVERS OF THE HERMITIAN CURVE

In Proposition 3.1, we write the degree of the ramification divisor R as the sum of $i(\sigma)$ for the $d - 1$ nontrivial σ in the Galois group G , and in Proposition 4.2 we found the possible values for each $i(\sigma)$. In particular, the nontrivial elements divide into two groups according to $i(\sigma) = 0, 1, 2, 3$ or $i(\sigma) = q^n + 1, q^n + 2$. Write $d = 1 + u + v$ with

$$u = \#\{\sigma \neq 1 : i(\sigma) = 0, 1, 2, 3\} \text{ and } v = \#\{\sigma \neq 1 : i(\sigma) = q^n + 1, q^n + 2\}.$$

Then

$$(5.1) \quad v(q^n + 1) \leq \deg R \leq v(q^n + 1) + 3u + v.$$

We compare this with the description of $\deg R$ in Section 2. For a subcover \mathcal{Y}_n of the Hermitian curve \mathcal{H}_n , not necessarily Galois, let $2g(\mathcal{Y}_n) - 2 = A(q^n + 1) - B$, with $1 \leq B \leq q^n + 1$, and let k be maximal with $k(A + 1) < B$. As in (2.3), let

$$(5.2) \quad \deg R = (2g(\mathcal{H}_n) - 2) - d(2g(\mathcal{Y}_n) - 2) = R_0(q^n + 1) + R_1,$$

where $R_0 = (q^n - 2 - dA + k)$ and $R_1 = dB - k(q^n + 1)$. Clearly,

$$(5.3) \quad k(R_0 - d) + (R_1 - d) \geq k(k - 3).$$

We will now prove a new lower bound for d .

Proposition 5.1. *Let \mathcal{Y}_n be a maximal curve with $2g(\mathcal{Y}_n) - 2 = A(q^n + 1) - B$, for integers A and B with $1 \leq B \leq q^n + 1$. For $B > A + 2$ and for $k(A + 1) < B$, if $\phi : \mathcal{H}_n \rightarrow \mathcal{Y}_n$ is a Galois covering of degree d then $dB \geq (k + 1)(q^n + 1)$.*

Proof. Assume to the contrary that $dB < (k + 1)(q^n + 1)$. Since $B \geq 2k + 1$, $3d < 2(q^n + 1)$, and thus $3u + v < 2(q^n + 1)$. With Lemma 2.1, $dB > dk(A + 1) \geq k(q^n + 1)$. Together with the assumption,

$$k(q^n + 1) < dB < (k + 1)(q^n + 1).$$

For $\deg R = R_0(q^n + 1) + R_1$ in (5.2), it follows that R_0 corresponds to the quotient and R_1 to the remainder after divisor by $q^n + 1$. Now we compare with (5.1). Using $R_0 \leq v + 1$ and $R_1 \leq 3u + v$,

$$k(R_0 - d) + (R_1 - d) \leq k(-u) + 2u - 1,$$

which, for $k \geq 3$, contradicts (5.3). It remains to prove the case ($k = 2$) and the case ($k = 1, B > A + 2$). Observe that for ($k = 1, B > A + 2$), (5.3) can be replaced with

$$(5.4) \quad (R_0 - d) + (R_1 - d) \geq d - 2.$$

If $3u + v < q^n + 1$ then $R_0 = v$ and $R_1 \leq 3u + v$. For ($k = 2$), $2R_0 + R_1 \leq 3u + 3v = 3d - 3$ contradicts (5.3). For ($k = 1, B > A + 2$), $R_0 + R_1 \leq 3u + 2v = 2d + u - 2$ contradicts (5.4). If $3u + v \geq q^n + 1$ then $R_0 \leq v + 1$ and $R_1 \leq 3u + v - 1$. For ($k = 2$), $2R_0 + R_1 \leq 3u + 3v + 1 = 3d - 2$. In combination with (5.3) equality holds and $R_0 = v + 1$ and $R_1 = 3u + v - 1$. The latter implies $3u + v = q^n + 1$, and $R_0 = v + 1$ would then

imply $R_1 = 0$, a contradiction. For $(k = 1, B > A + 2)$, $R_0 + R_1 \leq 3u + 2v = 2d + u - 2$ contradicts (5.4). \square

We will apply the above proposition to the generalized GK curve \mathcal{C}_n and the plane curve \mathcal{X}_n , that are both maximal curves over $\mathbb{F}_{q^{2n}}$. For their genera we have

$$(5.5) \quad \begin{aligned} 2g(\mathcal{H}_n) - 2 &= (q^n - 2)(q^n + 1), \\ 2g(\mathcal{C}_n) - 2 &= (q^2 - 1)(q^n + 1) - (q^3 + 1), \end{aligned}$$

$$(5.6) \quad 2g(\mathcal{X}_n) - 2 = (q - 1)(q^n + 1) - (q^2 + 1).$$

We first consider the generalized GK curve \mathcal{C}_n . Suppose now that $\phi : \mathcal{H}_n \rightarrow \mathcal{C}_n$ is a Galois covering of degree d . From (5.5), we have $A = q^2 - 1$, $B = q^3 + 1$ and $k = q$. Proposition 5.1 gives the lower bound for d as

$$d \geq \frac{(k+1)(q^n+1)}{B} = \frac{q^n+1}{q^2-q+1}.$$

From (2.1) we have the upper bound, for $n \geq 3$,

$$d \leq \frac{2g(\mathcal{H}_n) - 2}{2g(\mathcal{C}_n) - 2} \leq \frac{q^n - 2}{q^2 - 2}.$$

For $q \geq 3$ and $n \geq 3$ the lower bound exceeds the upper bound and no solutions for d exist. Hence the GK curve cannot be a Galois subcover of the Hermitian curve. This is Theorem 1.1.

For $q = 2$, $2g(\mathcal{H}_n) - 2 = (2^n + 1)/3 \cdot (2g(\mathcal{X}_n) - 2)$ and the inequalities admit the unique solution $d = (2^n + 1)/3$. This gives the degree in Theorem 1.2. Moreover, Proposition 3.1 reveals that such a covering, if it exists, has to be unramified. This proves Theorem 1.2.

Remark 5.2. In the proof we did not use the fact that we are dealing with the generalized GK-curve \mathcal{C}_n . What we use is only the genus of \mathcal{C}_n given by (5.5). Thus we actually prove that there are no curves with genus $\frac{1}{2}(q-1)(q^{n+1} + q^n - q^2)$ being a Galois subcover of the Hermitian curve \mathcal{H}_n when $q \geq 3$ and odd $n \geq 3$.

We now turn our attention to \mathcal{X}_n . Suppose that $\phi : \mathcal{H}_n \rightarrow \mathcal{X}_n$ is a Galois covering of degree d . From (5.6), we have $A = q - 1$, $B = q^2 + 1$ and $k = q$. Proposition 5.1 and (2.1) gives the lower and upper bounds for d as

$$\frac{(q+1)(q^n+1)}{q^2+1} \leq d \leq q^{n-1} + q^{n-2} + \dots + q^2 + q + 2.$$

This proves Theorem 1.3.

Remark 5.3. In most cases we expect that one need to incorporate our ideas with other methods to completely remove the possibility of a curve being a Galois subcover of the Hermitian curve. For a concrete example, consider $n = 3$. Then \mathcal{X}_3 is given by the equation $y^{q^2} - y = z^{q^2-q+1}$ and has genus $\frac{1}{2}(q-1)(q^3 - q)$. Our bounds for the degree d gives $q^2 + q \leq d \leq q^2 + q + 2$. We can eliminate the cases $d = q^2 + q + 1$ and $d = q^2 + q + 2$

by some elementary arguments. However, the case $d = q^2 + q$ is more subtle. It turns out that there is a curve

$$\mathcal{Y} : y^{q^2} - y^q + y = x^{q^2-q+1}$$

which has the same genus as \mathcal{X}_3 , and is a Galois subcover of the Hermitian curve of degree $q^2 + q$, with

$i(\sigma)$	0	1	2	3	$q^3 + 1$	$q^3 + 2$
$\#\sigma$	1	$q^2 - q$	0	0	q	$q - 1$

It can be proved by the same idea as the case $q = 3$ in [11] that \mathcal{Y} is not isomorphic to \mathcal{X}_3 , but that does not settle the case $d = q^2 + q$ completely.

Acknowledgments. We would like to express our gratitude to Professor Mike Zieve and Professor Rachel Pries for pointing out a mistake in an earlier version of the preprint.

REFERENCES

- [1] Miriam Abdón, Juscelino Bezerra, and Luciane Quoos, *Further examples of maximal curves*, J. Pure Appl. Algebra **213** (2009), no. 6, 1192–1196.
- [2] Miriam Abdón and Arnaldo Garcia, *On a characterization of certain maximal curves*, Finite Fields Appl. **10** (2004), no. 2, 133–158.
- [3] Miriam Abdón and Fernando Torres, *On maximal curves in characteristic two*, Manuscripta Math. **99** (1999), no. 1, 39–53.
- [4] Antonio Cossidente, Gabor Korchmáros, and Fernando Torres, *On curves covered by the Hermitian curve*, J. Algebra **216** (1999), no. 1, 56–76.
- [5] ———, *Curves of large genus covered by the Hermitian curve*, Comm. Algebra **28** (2000), no. 10, 4707–4728.
- [6] Iwan M. Duursma, *Two-point coordinate rings for GK-curves*, IEEE Trans. Inform. Theory **57** (2011), no. 2, 593–600.
- [7] Rainer Fuhrmann, Arnaldo Garcia, and Fernando Torres, *On maximal curves*, J. Number Theory **67** (1997), no. 1, 29–51.
- [8] Rainer Fuhrmann and Fernando Torres, *The genus of curves over finite fields with many rational points*, Manuscripta Math. **89** (1996), no. 1, 103–106.
- [9] Arnaldo Garcia, *Curves over finite fields attaining the Hasse-Weil upper bound*, European Congress of Mathematics, Vol. II (Barcelona, 2000), Progr. Math., vol. 202, Birkhäuser, Basel, 2001, pp. 199–205.
- [10] Arnaldo Garcia, Cem Güneri, and Henning Stichtenoth, *A generalization of the Giulietti-Korchmáros maximal curve*, Adv. Geom. **10** (2010), no. 3, 427–434.
- [11] Arnaldo Garcia and Henning Stichtenoth, *A maximal curve which is not a Galois subcover of the Hermitian curve*, Bull. Braz. Math. Soc. (N.S.) **37** (2006), no. 1, 139–152.
- [12] Arnaldo Garcia, Henning Stichtenoth, and Chao-Ping Xing, *On subfields of the Hermitian function field*, Compositio Math. **120** (2000), no. 2, 137–170.
- [13] Massimo Giulietti and Gábor Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. **343** (2009), no. 1, 229–245.
- [14] Daniel R. Hughes and Fred C. Piper, *Projective planes*, Springer-Verlag, New York, 1973, Graduate Texts in Mathematics, Vol. 6.
- [15] Yasutaka Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 721–724.
- [16] Gábor Korchmáros and Fernando Torres, *Embedding of a maximal curve in a Hermitian variety*, Compositio Math. **128** (2001), no. 1, 95–113.
- [17] ———, *On the genus of a maximal curve*, Math. Ann. **323** (2002), no. 3, 589–608.

- [18] Gilles Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C. R. Acad. Sci. Paris Sér. I Math. **305** (1987), no. 16, 729–732.
- [19] Vicente Landazuri and Gary M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443.
- [20] Heinrich-Wolfgang Leopoldt, *Über die Automorphismengruppe des Fermatkörpers*, J. Number Theory **56** (1996), no. 2, 256–282.
- [21] Hans-Georg Rück and Henning Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994), 185–188.
- [22] Jean-Pierre Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.
- [23] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.
- [24] Henning Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I, II*, Arch. Math. (Basel) **24** (1973), 527–544, 615–631.
- [25] ———, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.
- [26] Henning Stichtenoth and Chao Ping Xing, *The genus of maximal function fields over finite fields*, Manuscripta Math. **86** (1995), no. 2, 217–224.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, 273 ALTGELD HALL, MC-382, 1409 W. GREEN STREET, URBANA, ILLINOIS 61801, USA

E-mail address: `duursma@math.uiuc.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, 273 ALTGELD HALL, MC-382, 1409 W. GREEN STREET, URBANA, ILLINOIS 61801, USA

E-mail address: `mak4@illinois.edu`